Troyanos y gusanos: el reinado del malware

Análisis de las 100 amenazas más detectadas por ESET en Latinoamérica

ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Autor:
SebastiánBortnik
Coordinador de Awareness & Research

Fecha:
01 de mayo del 2011

Índice

Introducción

Virus, gusanos, troyanos, spyware, adware... todo parece ser confuso para los usuarios, que ante una infección, les resulta difícil comprender qué es lo que está atentando contra la seguridad de su información. Estadísticas revelan que durante el 2010, el 84% de los usuarios hogareños se infectaron al menos una vez; y cuatro de cada diez personas recurre al formateo de su computadora ante un incidente con códigos maliciosos. ¿Es esta la mejor opción? Aunque muchas veces en términos costo-beneficio suele serlo, hay otros dos motivos fundamentales que influyen en que la mitad de los usuarios infectados lleguen a esta decisión. En primer término, que no se poseen las medidas de prevención suficiente y, en segundo lugar, que muchas veces se desconoce la naturaleza de las amenazas que atentan contra el sistema, o que infectaron al mismo.

En ese contexto, ESET Latinoamérica ha realizado un análisis que pretende graficar el **estado de la seguridad en la región**, a partir de los códigos maliciosos más detectados durante el último año.

Para ello, se utilizaron las estadísticas de ThreatSense.Net, el sistema de alerta temprana de ESET, que permite conocer el estado de las detecciones de malware en todo el mundo. El presente informe, es el resultado del análisis de las **100 amenazas más detectadas por ESET en Latinoamérica**, durante el año 2010 (disponibles en el anexo de este documento).

¿Cuáles son los códigos maliciosos más detectados? ¿Qué es más probable, infectarse con un troyano, un gusano o un virus? Estas, y otras preguntas basadas en el comportamiento promedio de las amenazas en la región, serán respondidas a lo largo del documento, como así también se realizará un análisis y descripción de los cinco principales códigos maliciosos que infectaron el último año a usuarios de Latinoamérica.

Tipos de malware: ¿el fin de los virus?

Aunque los términos virus y malware suelen utilizarse para los mismos fines, vale destacar que no se trata del mismo concepto. Los virus informáticos son las amenazas que dieron origen a

esta problemática, mientras que, el malware (del inglés, *malicious software*, aplicación maliciosa) es el concepto que engloba a todos los tipos de amenazas informáticas, no solo los virus, sino también gusanos, troyanos, spyware, entre otros.

Por lo tanto, vale la pena analizar cómo están distribuidos los códigos maliciosos a partir de su tipo, es decir, virus, gusanos, troyanos, adware y spyware. Según las 100 amenazas más detectadas por ESET, la distribución de las mismas indica con claridad que los virus informáticos tienden a desaparecer, así como también los spyware tradicionales, tal como se muestra en la siguiente imagen:

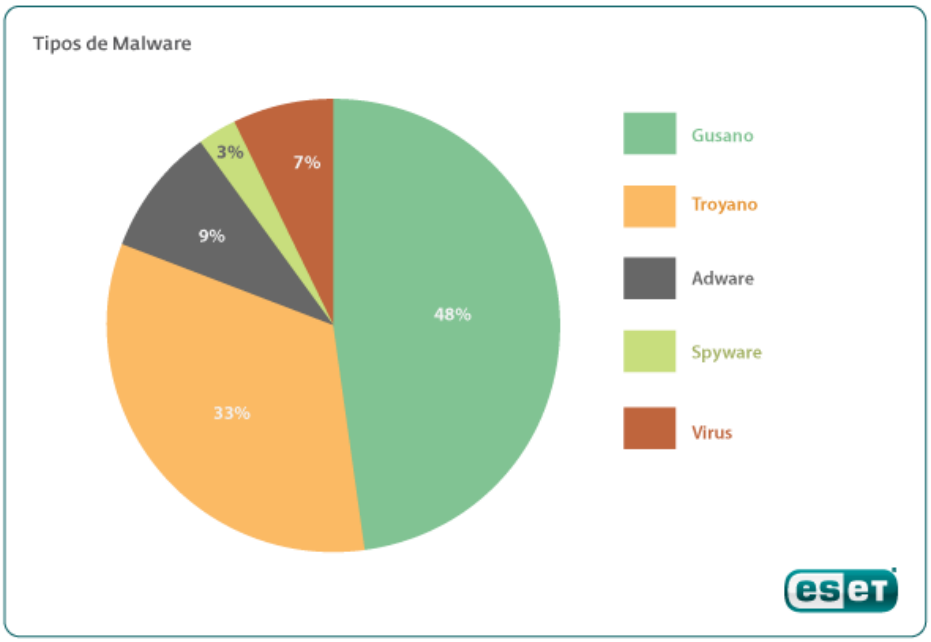

Imagen 1: Tipos de Malware actuales según ThreatSense.NET

Como se puede apreciar en la misma, los **virus informáticos** poseen poca relevancia en el escenario global de amenazas (tan solo el 7%). En este, los **gusanos (48%)** y los **troyanos (33%)** ocupan la mayoría de los códigos maliciosos propagados en la región. De hecho, dentro de las 100 amenazas más detectadas, recién en el vigésimo cuarto lugar aparece un virus informático, *Win32/FlyStudio.OGS* (24º). Por otro lado, entre los seis malware más detectados se identifican cuatro gusanos: *INF/Autorun* (1º), *Win32/Conficker.AA* (2º), *INF/Autorun.gen* (4º) y *Win32/Tifaut.C* (5º), y dos troyanos, *Win32/PSQ.OnLineGames.OUM* (3º) y *Win32/PSW.OnLineGames.NNU* (6º).

El **adware (9%)** y el **spyware (3%)** completan las variantes de amenazas, teniendo el primero de estos una mayor preponderancia, ya que ocupa el tercer lugar de malware más detectado. Estos, son códigos maliciosos diseñados para la exposición de publicidades no deseadas en el equipo del usuario. En esta categoría, que representa una de cada diez amenazas en la región,

aparecen también los rogue, falsos antivirus diseñados con el ánimo de estafar al usuario cobrando por una solución de seguridad ilegítima.

Finalmente, la baja tasa de amenazas del tipo spyware, viene dada por el **aumento de amenazas del tipo botnet** (ver sección siguiente). Mientras hace unos años estos códigos maliciosos, diseñados para robar información, eran efectivos para los atacantes, hoy en día esta acción suele ser llevada a cabo a través de redes de equipos zombis, conformadas por gusanos y troyanos, líderes de este ranking de códigos maliciosos.

Como se pudo observar, en la actualidad los virus informáticos han dejado el lugar protagónico a otras amenazas con características más efectivas para infectar ya que son más sencillas de desarrollar y son más funcionales para los ciber delincuentes de hoy en día.

¿Por qué los gusanos y troyanos tuvieron tal preponderancia? Particularmente se debe a que los métodos de propagación basados en **Ingeniería Social** o **explotación de vulnerabilidades** son las vías más efectivas para los atacantes, al momento de propagar masivamente sus códigos maliciosos. Estos, justamente, son los métodos utilizados por **gusanos y troyanos** que, según el TOP 100 del malware en la región, son las amenazas que más atentan contra los usuarios, los sistemas y, esencialmente, su información.

Características del malware

Una vez conocidos los tipos de códigos maliciosos más propagados, es importante profundizar, no sólo en las tipologías, sino también en sus características. Definir un malware no es una tarea sencilla, ya que es frecuente que una amenaza posea características de más de una variante. Un código malicioso puede propagarse por Ingeniería Social, y ser identificado como un troyano, y a la vez mostrar publicidad, lo que lo convierte al mismo tiempo en un adware. Aunque al momento de la clasificación priman los aspectos más relevantes de la amenaza, es importante tener en cuenta que conocer la distribución según el tipo de amenaza, es solo el primer paso.

Por lo tanto, más allá de su tipología, ¿Qué más se conoce sobre los códigos maliciosos más propagados en Latinoamérica? ¿Cuáles son sus características más importantes? A partir del ranking, se analizaron las cualidades más frecuentes del malware, y se describen las más relevantes a continuación.

Ingeniería Social

El 45% de las amenazas más detectadas según ThreatSense.Net usan Ingeniería Social. Es decir, que para su propagación, utilizan componentes sociales para engañar a los usuarios que, de una u otra forma, se convierten en cómplices involuntarios de la infección. En esta categoría, se incluyen troyanos como *Win32/PSW.Onlinegames* (3º, 6º, 18º, 72º y 97º, con distintas variantes), Win32/Peerfag (30º, 46º, 54º, 75º, 89º y 90º, con distintas variantes) o Win32/TrojanDownloader (43º, 64º, 65º, 69º, 80º y 94º, con distintas variantes), entre otras. Estos ejemplos marcan otra tendencia: las amenazas que utilizan Ingeniería Social son propensas a la multiplicidad de variantes, ya que a partir de un vector de propagación basado en engañar al usuario, se hace más factible para los atacantes crear diversas variantes.

El hecho de que la Ingeniería Social sea la característica que más se destaca entre las 100 amenazas más detectadas, deja muy en claro las necesidades en materia de concientización y educación en la región. Especialmente a partir de la costumbre de los atacantes de usar temáticas regionalizadas y locales con problemáticas o acontecimientos de países latinoamericanos, confirma la importancia de educar al usuario, para que no se exponga de forma desprevenida a estos códigos maliciosos.

Dispositivos USB y vulnerabilidades

La segunda característica que se destaca al analizar el ranking en cuestión (ver anexo), es la utilización de dispositivos USB para infectar sistemas con malware, cualidad identificada en el **41% de las amenazas**. Esta característica cobra mayor relevancia que otros años, teniendo en cuenta que Microsoft deshabilitó la ejecución automática de dispositivos externos a través de Autorun, en febrero de 2011 (más información en la KB971029). Sin embargo, a pesar de ello, no se ha observado una disminución de infecciones, dato que no resulta llamativo ya que las altas tasas de uso de software no licenciado en Latinoamérica hacen que gran parte de los usuarios no actualicen sus sistemas operativos.

Cuatro de cada diez usuarios conectaron un dispositivo USB infectado a sus computadoras durante el último año, y claramente es otra de las características preponderantes en Latinoamérica. El miedo a conectar un USB ajeno a un sistema propio es una constante para usuarios en la región, que consideran a este tipo de dispositivos como sinónimo de peligro, y están en lo correcto, tal como se evidencia en los primeros puestos del ranking presentado en este informe.

Finalmente, también se destaca que el **17% del malware explota vulnerabilidades**, lo cual junto al dato anterior, corrobora la importancia de los gusanos informáticos, que a pesar de existir en menos cantidad que los troyanos (que suelen tener más cantidad de variantes),

cuentan con índices de propagación mayores, especialmente cuando se trata de la explotación de vulnerabilidades.

Botnet

Continuando con las características distintivas del malware en Latinoamérica, se destacan en tercer lugar las botnet, redes de equipos zombis infectados, que son controlados remotamente por un atacante. Si se consideran también los troyanos del tipo *backdoor*, que incluyen una puerta trasera de acceso a los sistemas, uno de cada cinco códigos maliciosos del TOP 100 permite el control remoto de los equipos para actividades maliciosas.

Entre las acciones más utilizadas, es posible destacar el robo de información, los ataques de denegación de servicio o el envío de spam desde los equipos zombis. Tal como el equipo de ESET Latinoamérica pronosticara en el informe Tendencias 2011: las botnet y el malware dinámico, las redes botnet serán cada vez más utilizadas, y este porcentaje seguirá en crecimiento a lo largo de los próximos años.

Entre los códigos maliciosos más importantes del tipo botnet, ubicados en el ranking de amenazas (ver anexo) se destacan *Win32/Conficker* (5º, 7º y 60ª, según sus variantes), *IRC/SdBot* (el más popular de los administrador por IRC) y *Win32/Peerfrag* (30º, 46º y 75º, según sus variantes). Por otro lado, también se incluyen en esta categoría otras amenazas del tipo backdoor que, aunque no conforman lo que sería una red botnet, sí permiten al atacante ingresar remotamente al equipo infectado, tales como *Win32.Virut.NBP* (41º) o *Win32/Slugin.A* (48º).

Robo de información

Finalmente, para completar el cuadro de las características más importantes del malware en Latinoamérica, es necesario mencionar el robo de información. El 27% de los códigos maliciosos listados poseen algún tipo de rutina para robar datos del equipo infectado, como por ejemplo *Win32/PSW.OnLineGames.NNU* (6º), que envía al atacante las claves de acceso del usuario a juegos en línea como Lineage, World of Warcraft, Age of Conan, Cabal, Dekaron, Seal Online; entre otros.

Además, se destacan los troyanos bancarios, diseñados para obtener usuarios y claves de acceso a banca en línea, como *Win32/Qhost* (15º) o *Win32/Qhost.Banker.EM* (35º). Ambas amenazas utilizan técnicas de pharming local para redireccionar al usuario a sitios de phishing al momento de intentar acceder a un sitio de determinado banco.

El TOP 5

Completando la descripción de las amenazas más importantes de la región, vale analizar las cuatro familias de malware que se ubican en las primeras cinco posiciones de los códigos maliciosos más detectados según ThreatSense.Net

INF/Autorun (1º/4º)

Se trata de una de las firmas genéricas que posee ESET NOD32 Antivirus, para detectar códigos maliciosos que se propagan a través de dispositivos USB o memorias extraíbles, que poseen el archivo Autorun.inf, que es utilizado para la ejecución automática de la amenaza. El lugar ocupado por esta amenaza, se condice con lo indicado secciones anteriores: la alta tasa de uso de los dispositivos USB para la infección de sistemas en la región, y la incidencia de la falta de costumbre de los usuarios en mantener sus sistemas actualizados. Otra firma genérica que posee características muy similares, es *INF/Autorun.gen* (4º), cuyos vectores de propagación son exactamente los mismos. Un archivo autorun.inf que propaga malware, y que puede ser detectado por esta firma, se ve de la siguiente manera:

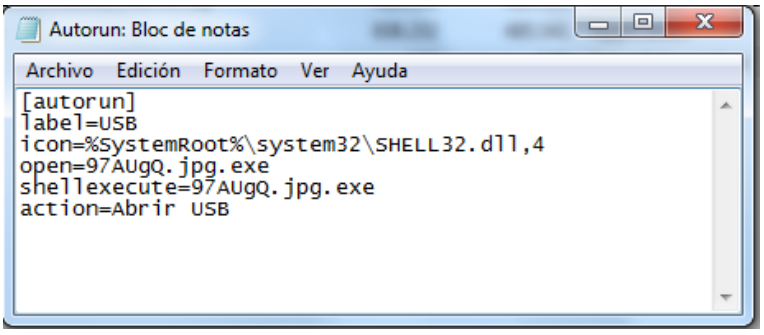

Imagen 2: Tipo de archivo Autorun.inf

Win32/Conficker.AA (2º)

Si hay un código malicioso que causó infecciones en todo el mundo, y con altos índices de infección, es el gusano Conficker. Este malware, que apareció en noviembre del año 2008, se propagaba a través de la explotación de la vulnerabilidad MS08-067, publicada por Microsoft (junto al parche correspondiente) el mes anterior. La misma, permitía la ejecución de código automática a través del protocolo RPC.

Win32/Conficker.AA (2º) es la primer variante de esta amenaza (luego aparecerían más versiones), publicada el 29 de diciembre del 2008. Conocida popularmente como Conficker.B, esta versión del gusano no solo podía propagarse a través de equipos en red con la vulnerabilidad, sino también a través de **dispositivos USB y carpetas compartidas** que tuviesen contraseñas débiles por medio de ataques de diccionario con una base de datos de 248 posibles contraseñas para acceder a recursos en otros sistemas.

Esta versión también incorporó rutinas para evitar su desinfección, cerrando procesos de los más reconocidos fabricantes de antivirus y bloqueando el acceso a sitios web en cuyos nombres hubiese cadenas específicas (por ejemplo, "windowsupdate", "eset" y "nod32"). Con la aparición de esta variante, los equipos que ya hubieran instalado el parche de seguridad de Microsoft MS08-067 también podrían infectarse a través de los nuevos mecanismos de propagación.

Esto explica por qué, esta variante del gusano es la más propagada, y hace que esta amenaza siga causando pérdidas económicas a lo largo de todo el mundo[1]. ¿Gusano? ¿Vulnerabilidades? ¿USB? Sin lugar a dudas, Conficker es referente en lo que respecta a amenazas en Latinoamérica, y no casualmente ocupa el segundo lugar en el ranking de amenazas.

Win32/PSW.OnLineGames.OUM (3º)

La familia de amenazas *Win32/PSW.OnLineGames* se caracterizan por estar orientadas, de una u otra forma (dependiendo de su variante), a generar daños en usuarios que utilicen juegos en sus computadoras, la mayoría de ellos en línea. Son una consecuencia de las nuevas funcionalidades que incluyen este tipo de juegos, que ahora permiten el acceso online, el uso de dinero virtual, y por ende abren el juego para ataques como el robo de información o incluso el fraude económico.

Esta variante en particular, se caracteriza por descargar otros códigos maliciosos una vez instalado en el sistema, a partir de órdenes recibidas, vía protocolo HTTP, desde otra computadora en Internet.

[1] En abril de 2009, el Instituto de Ciber Seguridad realizó un estudio al respecto, estimando que las pérdidas causadas por el gusano podrían alcanzar los 9100 mil millones de dólares.

Win32/Tifaut.C (5º)

Este código malicioso es un gusano que también se propaga a través de dispositivo removibles, creando un archivo cada vez que se conecta uno de estos con los nombres (aleatoriamente) *alokium.exe* y *random.exe*. Además, se crea el archivo *autorun.inf* correspondiente, y un archivo vacío de nombre *khq*. La amenaza posee conectividad a cuatro direcciones URL, y puede recibir instrucciones para realizar alguna de las siguientes acciones:

1. Crear entrada de registro
2. Borrar entradas de registro
3. Recuperar información del sistema operativo

Resulta interesante analizar esta amenaza a lo largo del mundo, ya que se puede observar cómo algunos países de Latinoamérica poseen los más altos índices de propagación, como puede observarse en la siguiente imagen:

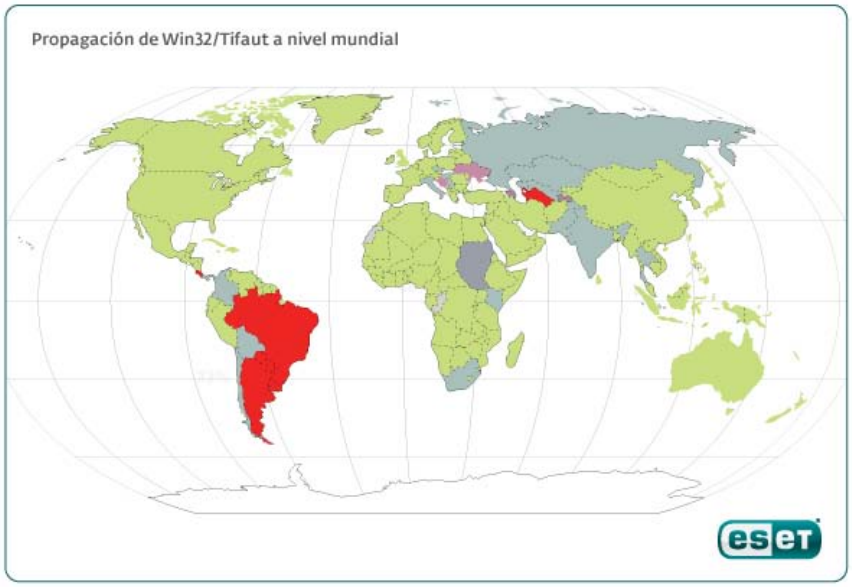

Imagen 3: Propagación de Win32/Tifaut a nivel mundial

Tifaut es un ejemplo de cómo el malware se ha comenzado a regionalizar, y archivos que pueden pasar prácticamente inadvertidos en algunas zonas del mundo, pueden ser de los más importantes en otras, como es el caso de Latinoamérica, y especialmente países como Argentina, Uruguay, Paraguay y Brasil.

Cuestión de familia

Más allá de las más populares, otras familias de amenazas tienen un protagonismo interesante en el listado, y aquí se deja una breve descripción de las más importantes:

Toolbars

Amenazas como *Win32/Toolbar.MyWebSearch* (19º), *Win32/Adware.Toolbar.Dealio* (29º), *Win32/Toolbar.AskSBar* (32º) o *Win32/Toolbar.MyWebSearch.K* (99º) son cada vez más propagadas en la región. Se trata de una serie de herramientas que, a pesar de simular ser inofensivas, y englobarse en un campo donde muchas lo son (las barras para agregar funcionalidades a los navegadores), muchas de ellas poseen funcionalidades del tipo adware o spyware, mostrando publicidades de forma indeseada al usuario, alterando los resultados de las búsquedas o robando información del sistema del usuario, también con fines publicitarios.

Peerfag

Seis variantes de este gusano aparecen en el ranking de amenazas. Se trata de un malware del tipo botnet, que según su variante puede propagarse por mensajería instantánea, o redes *peer-to-peer* (P2P).

Su propagación ha ido en aumento en Latinoamérica, y es utilizada para armar redes botnet, ya que posee la funcionalidad de enviar instrucciones al sistema infectado, que incluyen la descarga de archivos de Internet, y su posterior ejecución. Esto permite al atacante realizar cualquier instrucción que pueda ser programada en un archivo ejecutable.

Sality

Además de aparecer en tres variantes, la firma genérica de este virus polimórfico, *Win32/Sality* (33º) puede ser identificada en el ranking. El malware puede infectar todo tipo de procesos en ejecución bajo las extensiones EXE y SCR. Posee, además, rutinas para eliminar procesos de reconocidas empresas antivirus y de seguridad, como así también su bloqueo en el navegador web. Finalmente, posee cuatro direcciones URL desde las que descarga cualquier nuevo ejecutable disponible, y lo pone en ejecución.

TrojanDownloader

Se trata de códigos maliciosos que son solo el medio para otros códigos maliciosos. Estos archivos, al infectar un sistema, están diseñados para recibir instrucciones para descargar más ejecutables, que realizan diversas acciones dañinas en el equipo.

Virut

De comportamiento similar a Sality, *Win32/Virut.NBP* (41º) posee funcionalidades parecidas, aunque su comunicación para recibir instrucciones se realiza desde servidores IRC.

Conclusión: un camino lento

Estas son las características más importantes del malware en Latinoamérica, y las conclusiones más relevantes producto del análisis que se ha realizado del TOP10 obtenido a través de ThreatSense.NET.

No obstante, si se comparan los datos de todo el año 2010, junto con los datos estadísticos de abril de 2011, se puede concluir en que no existen grandes diferencias, más allá de pequeños cambios:

#	Malware	% de detección	Posición 2010
1º	INF/Autorun	5.09%	1º
2º	Win32/Conficker.AA	1.93%	2º
3º	INF/Autorun.gen	1.90%	4º
4º	Win32/PSW.OnLineGames.OUM	1.70%	3º
5º	Win32/Tifaut.C	1.66%	5º
6º	Win32/Conficker.X	1.46%	7º
7º	INF/Autorun.Sz	1.36%	---
8º	INF/Conficker	1.04%	8º

9º	Win32/Conficker.Gen	0.91%	10º
10º	Win32/PSW.OnLineGames.NNU	0.85%	6º

Es decir que, a pesar de haber transcurrido cuatro meses de comenzado el año, no se han notado cambios relevantes en las amenazas más propagadas en la región, como así tampoco en sus características.

Al observar la evolución del malware en Latinoamérica, es importante destacar dos cualidades esenciales, que son muy gráficas respecto a los atacantes, y las víctimas. En primer lugar, que las técnicas de infección basadas en gusanos, dispositivos USB y explotación de vulnerabilidades, siguen siendo las más utilizadas.

En segundo lugar, vale destacar que, a pesar de la aparición de códigos maliciosos emergentes, no se notan cambios radicales, y estos no logran tomar protagonismo. Los cambios del malware en Latinoamérica son lentos, y cuando un código malicioso logra altas tasas de infección, logra posicionarse por mucho tiempo como una seria preocupación en la región.

En resumen, en caso de que los usuarios no modifiquen sus conductas y optimicen la protección de sus sistemas, estos niveles de propagación seguirán ocurriendo. Más allá del trabajo de los creadores de malware, la seguridad que el usuario configure en su sistema, será la llave para lograr que al menos, este escenario se vuelva más complicado para los delincuentes informáticos quienes tendrán más obstáculos para atacar los equipos.

Anexo: el TOP100

#	Código malicioso	Porcentaje de detección	Tipo de malware
1	INF/Autorun	6.65	gusano
2	Win32/Conficker.AA	3.04	gusano
3	Win32/PSW.OnLineGames.OUM	2.36	troyano
4	INF/Autorun.gen	2.18	gusano
5	Win32/Tifaut.C	2.17	gusano
6	Win32/PSW.OnLineGames.NNU	1.90	troyano
7	Win32/Conficker.X	1.70	gusano
8	INF/Conficker	1.64	gusano
9	Win32/Conficker.AE	1.60	gusano
10	Win32/Conficker.Gen	1.24	gusano

#	Código malicioso	Porcentaje de detección	Tipo de malware
11	Win32/AutoRun.IRCBot.CX	1.21	gusano
12	JS/TrojanClicker.Agent.NAZ	0.96	troyano
13	Win32/Agent	0.95	troyano
14	Win32/MessengerPlus	0.93	adware
15	Win32/Qhost	0.84	troyano
16	Win32/AutoRun.KS	0.65	gusano
17	Win32/Packed.Autoit.Gen	0.64	troyano
18	Win32/PSW.OnLineGames.NMY	0.64	gusano
19	Win32/Toolbar.MyWebSearch	0.63	spyware
20	HTML/ScrInject.B.Gen	0.60	gusano
21	Win32/HackAV.G	0.56	troyano
22	Win32/Packed.FlyStudio.O.Gen	0.56	adware
23	Win32/Pacex.Gen	0.54	troyano
24	Win32/FlyStudio.OGS	0.54	virus
25	Win32/Bflient.K	0.51	gusano
26	Win32/Inject.NDO	0.49	troyano
27	IRC/SdBot	0.49	gusano
28	Win32/Genetik	0.48	troyano
29	Win32/Adware.Toolbar.Dealio	0.47	adware
30	Win32/Peerfrag.EC	0.46	gusano
31	Win32/Sality.NAR	0.45	virus
32	Win32/Toolbar.AskSBar	0.43	adware
33	Win32/Sality	0.43	virus
34	Win32/Adware.CiDHelp	0.39	adware
35	Win32/Qhost.Banker.EM	0.39	troyano
36	Win32/AutoRun.IRCBot.FC	0.38	gusano
37	Eicar [2]	0.38	
38	Win32/AutoRun.FlyStudio.PA	0.36	gusano
39	Win32/Adware.ADON	0.35	troyano
40	Win32/AutoRun.VB.RF	0.35	gusano

[2] Es un archivo diseñado para probar si una solución antivirus está funcionando en una computadora. A pesar de ser inofensivo, es detectado por todos los motores antivirus. Más información: http://eicar.org/anti_virus_test_file.htm

#	Código malicioso	Porcentaje de detección	Tipo de malware
41	Win32/Virut.NBP	0.34	virus
42	Win32/Adware.DoubleD	0.32	adware
43	Win32/TrojanDownloader.FakeAlert.ARF	0.29	spyware
44	Win32/AutoRun.VB.GJ	0.28	troyano
45	Win32/Autorun.FXT.Gen	0.27	gusano
46	Win32/Peerfrag.GW	0.27	gusano
47	Win32/AutoRun.VB.PU	0.25	gusano
48	Win32/Slugin.A	0.24	virus
49	Win32/Conficker.AK	0.23	gusano
50	Win32/Conficker.AB	0.23	gusano
51	Win32/Brontok.AQ	0.23	gusano
52	Win32/AutoRun.Agent.WF	0.23	gusano
53	Win32/Adware.FunWeb	0.22	adware
54	Win32/Peerfrag.FD	0.22	gusano
55	Win32/AutoRun.VB.GA	0.21	gusano
56	Win32/Packed.FlyStudio.P.Gen	0.21	troyano
57	Win32/Inject.NDR	0.21	gusano
58	Win32/Boberog.AZ	0.21	troyano
59	Win32/Sohanad.NEO	0.20	gusano
60	Win32/Conficker.AL	0.20	gusano
61	LNK/Exploit.CVE-2010-2568	0.20	gusano
62	Win32/VB.NMS	0.19	gusano
63	Win32/MCH	0.19	troyano
64	Win32/TrojanDownloader.FakeAlert.AQI	0.19	gusano
65	Java/TrojanDownloader.Agent.NBN	0.19	gusano
66	Win32/AutoRun.Agent.VR	0.18	troyano
67	Win32/HackKMS.A	0.18	troyano
68	Win32/Sality.NBA	0.18	gusano
69	WMA/TrojanDownloader.GetCodec.Gen	0.18	troyano
70	Win32/AutoRun.VB.UG	0.17	troyano
71	Win32/Adware.OneStep.F	0.17	adware
72	Win32/PSW.OnLineGames.NWF	0.17	troyano
73	Win32/SpamTool.Tedroo.AN	0.17	troyano
74	Win32/Sality.NAU	0.16	virus
75	Win32/Peerfrag.FJ	0.16	gusano
76	Win32/AutoRun.VB.RU	0.16	gusano

#	Código malicioso	Porcentaje de detección	Tipo de malware
77	Win32/Adware.GabPath.A	0.16	adware
78	Win32/AutoRun.VB.GG	0.16	troyano
79	Win32/KillProc.A	0.16	troyano
80	JS/TrojanDownloader.Pegel.BR	0.16	troyano
81	Win32/Packed.Autoit.E.Gen	0.16	troyano
82	HTML/Iframe.B.Gen	0.15	gusano
83	Win32/AutoRun.Agent.YO.Gen	0.15	troyano
84	Win32/AutoRun.Agent.EF	0.15	gusano
85	Win32/AutoRun.VB.RT	0.15	gusano
86	Win32/Conficker.A	0.15	gusano
87	Win32/AutoRun.VB.GE	0.15	gusano
88	Win32/AutoRun.JO	0.15	gusano
89	Win32/Peerfrag.CU	0.14	gusano
90	Win32/Peerfrag.DJ	0.14	gusano
91	Win32/AutoRun.VB.MA	0.14	gusano
92	Win32/AutoRun.VB.RE	0.14	gusano
93	Win32/BHO.NMM	0.14	troyano
94	Win32/TrojanDownloader.Agent	0.14	troyano
95	Win32/Alman.NAB	0.14	virus
96	Win32/Kryptik.FZG	0.14	troyano
97	Win32/PSW.OnLineGames.ODJ	0.13	troyano
98	Win32/Statik	0.13	troyano
99	Win32/Toolbar.MyWebSearch.K	0.13	spyware
100	Win32/VB.NRJ	0.12	troyano